Virginia Information Technologies Agency
VITA Cyber Security Tips
expect the best
August 2006 Vol. 1, No. 3

Erasing information and disposal of media

Protecting confidential and sensitive data from accidental disclosure is very important, and we all should strive to properly erase data and the disposal of media. Recent events in the news have shown what can happen when such data is disclosed. Wells Fargo, the Veterans Administration, the U.S. Navy, AOL, Bank of America, the City of Hampton, and the State of New York all have been in the news in the past several months for inadequately protecting personal data. What can we do to avoid the same problem.

How can I be sure files are erased?

Data can be stored electronically in multiple formats and locations. Data sometimes includes sensitive documents or may contain personally identifiable information, such as a Social Security number, credit card information or health-related information. The initial information may arrive on a CD and then be copied to the computer's hard drive and subsequently backed up for disaster recovery purposes. In this example, there are three different storage mediums: CD, hard drive and backup media. In addition, just viewing a file stored on a CD can create a temporary image of the information on the computer's hard drive as well.

Deleting files does not erase the information. It only makes the space containing the files available to store additional data. The information often can be retrieved by using forensics or other recovery tools. As new computers are purchased, older computers may be sold or surplused. You should assume that sensitive information may have been stored or viewed on all computers at some point in time. Before discarding your computer or portable storage devices, you need to be sure that that data has been erased or "wiped."

What type of 'wiping' program should be used?

Read/writable media (including your hard drive) should be "wiped" using software specified in the state standard "Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media," ITRM Standard SEC2003-02.1. Software that meets this standard is listed on the VITA Web site at http://www.vita.virginia.gov/docs/pubs/removingData.cfm.

Issues to be aware of when wiping data include:

- The wiping software must to be used correctly with all the appropriate options and switches set properly.
- It may take a long time to rewrite the drive or media.
- A defective drive cannot be wiped.
- Wiping a state-owned or locality owned computer hard drive should be performed by someone knowledgeable in the process and the standard rather than the end user.
- End users should be aware of the process to protect their own data on their home computers.

What about 'Write Once' media?

Certain media can be read many times but can only be written once. This type of media, usually CD's or DVD's, cannot be overwritten to ensure the erasure of sensitive information. Therefore, this type of media should be physically destroyed. Certain types of shredders are capable of shredding CD's and DVD's. If this type of shredder is not available, then safely breaking the device into four or more pieces would be an appropriate destruction measure.

I've heard of 'degaussing,' but what is it?

Degaussing is the erasure of information through the use of a very strong magnet and generally is used for erasing of diskette and magnetic tape media. This latter type of storage media is utilized by organizations with large data processing operations.

Can I just physically destroy the storage media?

Yes. Media that does not need to be re-used can be, and probably should be, physically destroyed. Media that contains sensitive or private data that can not be "wiped" should be physically destroyed.

What about a defective drive that is under warranty?

Most warranties require the buyer to return the defective drive to the vendor in order for a replacement to be provided. Check to be sure that your vendor has a policy requiring "defective" drives to be physically destroyed. There have been reports that these drives sometimes are fixed and resold without the removal the data. Be careful in these situations. Balance the risk of information being compromised versus the cost of the hard drive.

Please note that for all electronic storage media subject to the Commonwealth of Virginia ITRM standard is required to have Commonwealth data properly removed prior to disposal or release.

Do these procedures suggested for business and home computers?

Yes. However, businesses should maintain a log of all devices that have been erased/disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), destruction method used, and disposal method (such as sold, crushed, or shredded).

These tips are brought to you in the Commonwealth of Virginia by the
Virginia Information Technologies Agency (VITA) and the Virginia Office of Commonwealth Preparedness
in coordination with:

MS-ISAC

www.msisac.org

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM